

SKJERVEN  
MORRILL  
MACPHERSON  
FRANKLIN  
& FRIEL LLP

Docket No.: M-7916 US

December 9, 1999

Box Patent Application  
Assistant Commissioner for Patents  
Washington, D. C. 20231

Enclosed herewith for filing is a patent application, as follows:

Inventor(s): Fry, Steven; Sarkar, Shantanu

Title: Method And Apparatus For Bridged Telnet To IP Devices Through A Firewall

<u>X</u>	Return Receipt Postcard
<u>X</u>	This Transmittal Letter (in duplicate)
<u>17</u>	page(s) Specification (not including claims)
<u>25</u>	page(s) Claims
<u>1</u>	page Abstract
<u>3</u>	page(s) Declaration For Patent Application and Power of Attorney
<u>9</u>	Sheet(s) of Drawings
<u>1</u>	page(s) Recordation Form Cover Sheet (in duplicate)
<u>2</u>	page(s) Assignment

**CLAIMS AS FILED (fees computed under §1.9(f))**

For	Number Filed		Number Extra		Rate		Basic Fee
Total Claims	102	-20 =	82	x	\$18.00	=	\$ 1,476.00
Independent Claims	15	-3 =	12	x	\$78.00	=	\$ 936.00
<input type="checkbox"/> Application contains one or more multiple dependent claims ( total fee)							\$
<input type="checkbox"/> Fee for Request for Extension of Time							\$

Please make the following charges to Deposit Account 19-2386:

- |                                     |  |             |
|-------------------------------------|--|-------------|
| <input checked="" type="checkbox"/> | Total fee for filing the patent application in the amount of   | \$ 3,172.00 |
| <input checked="" type="checkbox"/> | The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account 19-2386. |             |

EXPRESS MAIL LABEL

NO:

EL252928635US

Respectfully submitted,

*Sam M Campbell*  
Sam Campbell  
Attorney for Applicant(s)  
Reg. No. 42,381

25 Metro Drive, Suite 700  
San Jose, CA 95110  
Phone 408 453-9200  
Fax 408 453-7979

Austin, TX  
Newport Beach, CA  
San Francisco, CA

"Express Mail" mailing label number:

EL252928635US

## METHOD AND APPARATUS SUPPORTING NETWORK COMMUNICATIONS THROUGH A FIREWALL

Fry, Steven G.  
Sarkar, Shantanu

### BACKGROUND OF THE INVENTION

#### Field of the Invention

The present invention relates to computer networks, and, more particularly, to  
10 a method and apparatus for allowing network communications to proceed between  
two computers despite the fact that one or both of the computers are protected by a  
firewall.

#### Description of the Related Art

As the Internet has grown, security concerns have grown as well. In order to  
15 prevent unauthorized access to computer systems connected to the Internet, gateway  
systems commonly referred to as firewalls have been developed in order to prevent  
such unauthorized access.

Fig. 1 illustrates a network architecture 100 that employs such security  
measures. A computer system 105 is coupled to a firewall system 110 that allows  
20 access to a network 115. Also coupled to network 115 by a firewall system 120 is a  
computer system 125. Preferably, firewall systems 110 and 120 allow computer  
systems 105 and 125 transparent access to network 115, respectively, but prevent  
access to their respective computer systems originating from network 115. Thus,  
computer systems 105 and 125 are able to access other computer systems coupled to  
25 network 115 (e.g., a computer system 130). Such access may be accomplished by, for  
example, programs 135 and/or 140 accessing data 145 on computer system 130 using

any one of a number of networking protocols, as illustrated by connections 131 and 132. In contrast, firewall systems 110 and 120 prevent access to computer systems 105 and 125, respectively, by other systems coupled to network 115 (e.g., programs running on computer system 130 (not shown)).

5           Firewalls such as firewall systems 110 and 120 normally control access to the computers thus protected by controlling the ability to create connections to and from the computers they protect. Firewall systems 110 and 120 are thus configured to allow computer systems 105 and 125, respectively, to initiate connections to systems on the opposite side of their respective firewalls, but prevent the computer systems on  
10 the opposite side from initiating connections to the computers protected by the firewalls.

          However, it is often desirable to gain access to a system protected by a firewall from a system on the unprotected side of the firewall (also commonly referred to as the “dirty” side of a firewall). Because this type of access to a protected computer  
15 system is exactly that which a firewall is meant to prevent, the presence of a firewall impeded such access. For example, such is the case where a technical support group requires access to a customer’s computer system. If both the customer’s system and that of the technical support group are connected to a network, a desirable method of accessing the customer’s system would be via that network. Traditional solutions to  
20 this dilemma include supporting the desired communications via the use of an alternate communications path (exemplified by a connection 146), or the disabling of either the customer’s firewall or that of the technical support group (exemplified by a connection 147).

          The former solution is illustrated in Fig. 1, where modems 145 and 150 allow  
25 computer systems 105 and 125 to communicate via a public telephone system 155. A similar alternative is to configure computer systems 105 and 125 to communicate using a private network. The latter solution of simply disabling the firewall can be used to permit an outside computer (e.g., in the case of computer system 105, computer systems 125 or 130) to access the formerly-protected computer system.

Unfortunately, these solutions are less than ideal. Using an alternate communication system entails the additional costs of the alternate communication system and the need to commit valuable resources to the alternate system's installation and maintenance, among other such concerns. For example, when

5 implementing the alternate communication system shown in Fig. 1, modems 150 and 155 must be purchased and then connected to computer systems 105 and 125, respectively, as well as coupled to one another via public telephone system 160. This requires the operator of computer system 125 to arrange access to computer system 105 by some means and further requires that a modem-compatible connection be

10 made available for their use. Thus, access to computer system 105 by computer system 125 using an alternate means of communication is both inconvenient and raises issues of compatibility.

On the other hand, defeating the security features of firewall system 110 to allow access to computer system 105 by computer system 125 opens computer system

15 105 to attack by any computer system attached to network 115. When put in such a state, computer system 105 thus becomes susceptible to computer hackers, computer viruses and the like. As a result, access by this method is likely not available on an immediate basis, requiring the authorization of the management of the company to which computer system 105 belongs. Moreover, such a method is often awkward due

20 to the need for monitoring of the incoming data stream to prevent attacks on computer system 105 such as those mentioned previously. Given the foregoing issues and the need to access computer systems protected by a firewall, the ability to access a computer system through a firewall protecting that computer system would be of great use. Such a technique should be able to support the requisite communications without

25 the use of an alternate means of communication, and without the need to inhibit the firewall's security features.

### **Summary of the Invention**

The present invention, in various embodiments, addresses the aforementioned problems by providing techniques for allowing communication between computers

30 coupled to one another, possibly via a network, despite the fact of one or both

computers are protected by a firewall. Embodiments of the present invention allow such communication without the need for an alternative communications path (e.g., telephone communications). Such communications are supported by employing modes of communication permitted by the firewall(s), and coupling these permitted

5 connections to create an end-to-end connection that provides communication in the manner of a single communications path.

In one embodiment of the present invention, a method of communicating information between a first program and a second program over a network is described. The method includes relaying the information between the first program

10 and a first communications program over a first network connection, relaying the information between the first communications program and a second communications program over a second network connection and relaying the information between the second communications program and the second program over a third network connection. Further, the first communications program creates the second network

15 connection to the second communications program through a first firewall program, which prevents access to the first program initiated by the second program. Thus, the second network connection is initiated by the first communications program. As will be discussed, the first communications program can be, for example, a protocol daemon and the second communications program can be, for example, a relay

20 program. The first firewall program can also be configured to prevent access to the first program initiated by the second communications program.

In certain aspects of the method, the first program requires the first network connection to be initiated as an in-bound network connection relative to the first program. That being the case, the first network connection is initiated by the first

25 communications program as an in-bound connection relative to the first program. Further, the first firewall program can be configured, for example, to prevent access to the first program by preventing an in-bound network connection to the first program, the in-bound network connection being in-bound relative to the first program. In that case, the second network connection can be created, for example, as an out-bound

30 network connection from the first communications program to the second

communications program. The third network connection can be created, for example, through a second firewall program that prevents access to the second program initiated by the second communications program. In that case, the third network connection is initiated by the second program. In one aspect of the embodiment, the second firewall program prevents access to the second program by inhibiting an in-bound network connection to the second program (relative to the second program).

In another embodiment of the present invention, a method of communicating information between a first program and a second program over a network is described. The method includes relaying the information between the first program and a first communications program (which can be, for example, a relay program) over a first network connection and relaying the information between the first communications program and the second program over a second network connection. In this embodiment, the first program creates the first network connection to the first communications program through a first firewall program, which prevents access to the first program initiated by the second program. The first network connection is therefore initiated by the first program in such a configuration.

In yet another embodiment of the present invention, a method of communicating information over a network is described. The method includes relaying the information between a first program and a first communications program over a first network connection and relaying the information between the first communications program and a second program over a second network connection. In this embodiment, the first program requires the first network connection to be initiated as an in-bound network connection relative to the first program. Thus, the first network connection is initiated by the first communications program and is in-bound relative to the first program. Further, the first communications program creates the second network connection to the second program through a first firewall program that prevents access to the first program initiated by the second program. The second network connection is therefore initiated by the first communications program. The first communications program can be, for example, a protocol daemon.

5 A network according to one embodiment of the present invention includes a first program executed on a first computer, a first firewall program executed on a second computer coupled to the first computer, a second program executed on a third computer coupled to the second computer and a third program executed on a fourth computer coupled to the third computer. In this embodiment, the first firewall program is configured to prevent access to the first program initiated by the third program, while the first program is configured to initiate a first network connection to the second program through the first firewall program. The second program and the third program are also configured to support a second network connection between the second program and the third program. A second firewall program may also be included in the network, and is executed on a fifth computer coupled between the third computer and the fourth computer, if so provided. The second firewall program can be configured, for example, to prevent access to the third program initiated by the first program. Further, the first firewall program can also be configured to prevent access to the first program initiated by the second program, while the second firewall program can also be configured to prevent access to the third program initiated by the second program.

20 In one aspect of the embodiment, a fourth program, executed on a fifth computer coupled to the first computer, is provided as part of the network. The first program can then be configured to initiate a third network connection to the fourth program. In such a case, the fourth program is configured to require the third network connection to be initiated as an in-bound network connection relative to the fourth program. The third network connection is therefore an in-bound connection relative to the fourth program. Further, the first firewall program can be configured to prevent access to the first and the fourth programs by preventing in-bound network connections to the first and the fourth programs. In that case, the first network connection is created as an out-bound network connection from the first program to the second program.

30 The foregoing is a summary and thus contains, by necessity, simplifications, generalizations and omissions of detail; consequently, those skilled in the art will

appreciate that the summary is illustrative only and is not intended to be in any way limiting. Other aspects, inventive features, and advantages of the present invention, as defined solely by the claims, will become apparent in the non-limiting detailed description set forth below.

## 5 **BRIEF DESCRIPTION OF THE DRAWINGS**

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

Fig. 1 is a block diagram illustrating a network architecture of the prior art.

10 Fig. 2 is a block diagram illustrating a network architecture according to one embodiment of the present invention.

Fig. 3 is a flow diagram illustrating the actions performed by a protocol daemon according to one embodiment of the present invention.

15 Fig. 4 is a flow diagram illustrating the actions performed by a relay program according to one embodiment of the present invention.

Fig. 5 is a flow diagram illustrating an overall process for relaying information between programs according to one embodiment of the present invention.

20 Fig. 6 is a flow diagram illustrating an overall process for relaying information between programs according to one embodiment of the present invention that employs a password protocol.

Fig. 7 is a block diagram illustrating a network architecture according to another embodiment of the present invention.

25 Fig. 8 is a flow diagram illustrating an overall process for relaying information between programs according to an embodiment of the present invention such as that of Fig. 7.



The use of the same reference symbols in different drawings indicates similar or identical items.

## **DETAILED DESCRIPTION OF THE INVENTION**

The following is intended to provide a detailed description of an example of the invention and should not be taken to be limiting of the invention itself. Rather, any number of variations may fall within the scope of the invention which is defined in the claims following the description.

Fig. 2 is a block diagram illustrating one embodiment of a network architecture 200 according to the present invention. As with network architecture 100 of Fig. 1, program 140 cannot initialize communications with program 135 and, conversely, program 135 cannot initialize communications with program 140 while both firewall 110 and firewall 120 are operational. This is because firewalls 110 and 120 allow outgoing connection initialization, but do not allow the initialization of connections on an in-bound basis. By allowing only outbound connections (and preventing inbound connections), firewalls 110 and 120 effectively reduce the opportunity for outside entities (e.g., “hackers”) to infiltrate computer systems 105 and 125. As will be apparent to those of skill in the art, the firewalls described herein may employ other measures (similar in effect to those just described) to prevent unauthorized access to computers protected by those firewalls, and such alternative techniques are intended to be comprehended by the methods discussed herein.

In order to support a connection between programs 135 and 140, network architecture 200 includes a relay program 210 running on a computer system 220. Such connections can employ, for example, the TCP/IP protocol to support Telnet connections between the various entities. As can be seen in Fig. 2, computer system 220 is coupled between firewall 120 and network 115, although computer system 220 could be coupled directly to firewall 110, or coupled between firewall 110 and network 115 with no substantive effect on the methods disclosed herein. Moreover, given software implementations (i.e., software programs) of the various functionalities described herein, it will be apparent to one of skill in the art that such programs may

be distributed in various ways among one or more computers for execution. Relay program 210 acts to couple two in-bound connections to one another using the protocol employed by the two in-bound connections. Such a situation is illustrated in Fig. 2 by the initiation of an out-bound connection 230 from program 140 to relay program 210, and an out-bound connection 240 from program 135 to relay program 210. The process of making such a connection is described in further detail below with regard to Fig. 5a.

In the case where program 135 requires an in-bound connection (e.g., where program 135 is an application server), the inventors determined that some way to provide the in-bound connection required by program 135 and an out-bound connection to relay program 210 must be provided. Such functionality can be supported by providing a program capable of initiating the required connections. Such a program resides on the protected side of firewall 110 in order to initiate the requisite out-bound connection through firewall 110 in the stead of such a connection from program 135.

The requisite functionality may be provided, for example, by a daemon running on computer system 105. Such a daemon is illustrated in Fig. 2 as a protocol daemon 250. Such connections can employ, for example, the TCP/IP protocol to support Telnet connections between the various entities. Protocol daemon 250 initiates a in-bound connection to program 135 (illustrated in Fig. 2 as an internal connection 260). Protocol daemon 250 also initiates an out-bound connection 270 to relay program 210, via an out-bound port on firewall 110, in keeping with the paradigm supported by firewalls 110 and 120, although other protection techniques and alternative communication paths supported therein can be supported by embodiments according to the present invention. As before, program 140 initiates out-bound connection 230 to relay program 210. Relay program 210 then couples out-bound connections 230 and 270, relaying data between the two until such time as one of the connections either fails or is disconnected. From a conceptual standpoint, this coupling can be viewed as simply relaying data from one connection to another, or coupling the connections into a single connection. For added security, relay

program 210 may require in-bound connections (i.e., out-bound connections 230 and 270) to provide a password that can be used to authenticate the connections and so avoid unauthorized access to either of computer systems 105 and 125. Optionally, the password can be subjected to bit manipulation (e.g., encoding) in order to make the password unreadable during transmission.

Fig. 3 is a flow diagram illustrating operations performed by protocol daemon 250, should the use of such a protocol daemon be required to support connections between program 135 and entities on the "dirty" side of firewall 110. Such connections can employ, for example, the TCP/IP protocol to support Telnet connections between the various entities. When run, protocol daemon 250 creates a connection to program 135, illustrated in Fig. 3 as creating a connection to the server (step 300). If the connection is not successfully created (step 310), the attempted connection and all other pending, related connections are closed down (step 320). Alternatively, other connections may be left in place to await another connection request. If the connection is successfully created, protocol daemon 250 then attempts to create a connection to relay program 210 (step 320). Again, if the connection to relay program 210 is not successfully created (step 330), the attempted connection and all pending, related connections are closed down (step 320) (or the pre-existing connections ignored).

If a connection is successfully created to relay program 210 (represented in Fig. 2 as out-bound connection 270), data is relayed between program 135 and relay program 210 by protocol daemon 250 (step 340). This relaying of data continues until one of the two connections either fails or is disconnected (step 350), at which time the remaining connections are closed down (step 320). As will be apparent to one of skill in the art, the exact order of connection initialization is not critical, and so protocol daemon 250 can initiate either internal connection 260 or outbound connection 270 before the other without any substantive effect on the methods disclosed herein.

Each of the blocks of the flow diagram of Fig. 3, and those depicted in subsequent figures, may be executed by a module (e.g., a software module) or a

portion of a module or a computer system user. The methods described herein, the operations thereof and modules for performing such methods may therefore be executed on a computer system configured to execute the operations of the method and/or may be executed from computer-readable media. The method may be embodied in a machine-readable and/or computer-readable medium for configuring a computer system to execute the method. The software modules may be stored within and/or transmitted to a computer system memory to configure the computer system to perform the functions of the module.

Those skilled in the art will also recognize that the boundaries between modules and operations depicted herein are merely illustrative and alternative embodiments may merge such modules or operations, or impose an alternative decomposition of functionality thereon. For example, the actions discussed herein may be decomposed into sub-operations to be executed as multiple computer processes. Moreover, alternative embodiments may combine multiple instances of a particular operation or sub-operation. Furthermore, those skilled in the art will recognize that the operations described in exemplary embodiment are for illustration only. Operations may be combined or the functionality of the operations may be distributed in additional operations in accordance with the invention.

Fig. 4 is a flow diagram illustrating an exemplary set of operations that relay program 210 performs in supporting a connection between either of program 135 or protocol daemon 250, and program 140. Such connections can employ, for example, the TCP/IP protocol to support Telnet connections between the various entities. The exemplary process of Fig. 4 begins with the creation of a socket (step 400) for use by an in-bound connection. While the networking concept of a socket is employed in describing relay program 210, it will be apparent to one of skill in the art that the network connections referred to herein will be cast in terms of other programmatic constructs, and in fact, the appropriate construct will depend on the protocol being supported by the given embodiment of the present invention. These other programmatic constructs may be employed by such embodiments without deviating from the invention.

Upon the receipt of an in-bound connection requisition (step 410), a list of currently open sockets maintained by relay program 210 is searched in an effort to locate an open socket having a matching password (step 420). It will be noted that the process illustrated in Fig. 4 is one that uses passwords for each connection in order to provide enhanced security. Although passwords need not be employed, some method of determining which in-bound connections are to be coupled to other in-bound connections should be supported by relay program 210. Other such methods may include, for example, the use of network addresses, the use of verification strings (wherein a connection is attempted and only maintained upon the receipt of an alphanumeric string that verifies that the connection had been made by an authorized network element), and the like.

If the password provided does not match any of the current open sockets (step 430), relay program 210 makes the determination as to whether the attempted connection should be configured as a listening connection (step 440). If the requested connection is not to be left open in an effort to listen for a corresponding connection, the attempted connection is disconnected (step 450) and, if any, remaining connections are terminated (step 460). If the attempted connection is to be configured as a listening connection, the attempted connection is put on the list of currently open sockets (step 470).

Conversely, if the password of the attempted connection matches one or more of the currently open sockets, the end points are connected by relay program 210 (step 480). Once connected, relay program 210 relays data from one end point to the other end point (i.e., programs 135 and 140 of Fig. 2) (step 490). This relaying of data continues until one (or both) of the connections either fails or is disconnected (step 495), at which time all of the related connections are terminated (step 460).

Fig. 5A is a flow diagram illustrating a process according to one embodiment of network architecture 200 in which relay program 210 relays data between programs 135 and 140 without the use of a protocol daemon. The exemplary process begins with the execution of relay program 210 (step 500). Program 135 then creates a

connection to relay program 210 by initiating out-bound connection 240 through firewall 110 to relay program 210 (step 505). If program 135 is unsuccessful in creating outbound connection 240 (step 510), the attempted connection is terminated (step 515). If out-bound connection 240 is successfully created, program 140 then  
 5 attempts to create a connection to relay program 210 through firewall 120, illustrated in Fig. 2 as out-bound connection 230 (step 520). If the creation of out-bound connection 230 is unsuccessful (step 525), the attempted connection is terminated, as before (step 515). On the other hand, if the creation of out-bound connection 230 is successful, relay program 210 begins relaying data between programs 135 and 140  
 10 (step 530). The relaying of data between programs 135 and 140 continues until out-bound connection 230 and/or out-bound connection 240 is either disconnected or fails (step 535). Once one or both of these connections have failed or been disconnected, any remaining connections are terminated (step 515).

Fig. 5B is a flow diagram illustrating a process for communicating data  
 15 between programs 135 and 140 in the case where program 135 requires an in-bound connection. The exemplary communications process of Fig. 5B begins with the execution of protocol daemon 250 on computer system 105 (step 540). Next, relay program 210 is initiated on computer system 220 (step 545). Protocol daemon 250 then attempts to create a connection to program 135 (illustrated in Fig. 2 as internal  
 20 connection 260) (step 550). If internal connection 260 is not successfully created (step 555), all pending, related connections are terminated in order to avoid leaving open any connections related to the failed connection attempt, which is normally the desired case (step 560). It will be apparent to one of skill in the art, however, that one or more of the remaining connections can be left open, if desired.

25 If internal connection 260 is successfully created, protocol daemon 250 then attempts to create a connection to relay program 210 via firewall 110 and network 115 (step 565). As before, if this connection (depicted in Fig. 2 as out-bound connection 270) is not successfully created (step 570), any pending, related connections are terminated (step 560). If out-bound connection 270 to relay program 210 is  
 30 successfully created, program 140 then attempts to create a connection to relay

program 210 (depicted in Fig. 2 as out-bound connection 230) (step 575). Once again, if out-bound connection 230 is not successfully created (step 580), the attempted connection is terminated (step 560).

As will be apparent to one of skill in the art, although the initialization and execution of the various programs involved and the initialization of connections between those programs are depicted in Figs. 5A and 5B as occurring in a specific sequence, and are described in that manner, their actual order has no substantive effect on the operation of a network architecture according to an embodiment of the present invention. That being the case, for example, out-bound connection 240 (or out-bound connection 270) can be initiated before or after the initiation of out-bound connection 230. Once a connection from program 140 to relay program 210 is initiated, data may be relayed between programs 135 and 140 by protocol daemon 250 and relay program 210 (step 585). This relaying of data continues until one or both of out-bound connections 230 and/or 270 either fail or are disconnected (step 590), at which time any remaining connections are terminated (step 560).

Fig. 6 is a flow diagram illustrating the overall process of using relay program 210 and protocol daemon 250 to create a connection between programs 135 and 140 through firewalls 110 and 120. It will also be noted that the process of Fig. 6 employs passwords both to identify the proper connections to be made and provide an additional level of security. The process of creating such a connection begins with the execution of protocol daemon 250 on computer system 105 (step 600) and the initiation of relay program 210 on computer system 220 (step 605). Next, protocol daemon 250 attempts to create a connection to program 135 (depicted in Fig. 2 as internal connection 260) (step 610). If the creation of internal connection 260 is unsuccessful (step 615), the attempted connection is terminated (step 620). If internal connection 260 is successfully created, a password for use in connecting to relay program 210 is provided to protocol daemon 250 (step 625). Protocol daemon 250 then attempts to create a connection to relay program 210 (depicted in Fig. 2 as out-bound connection 270) using the password provided (step 630). As before, if out-bound connection 270 cannot be successfully created (step 635), the attempted

connection and any other related connections are terminated (step 620). If the connection from protocol daemon 250 to relay program 210 is successfully created, the password/connectivity list of relay program 210 is updated (step 640).

Next, a password corresponding to that given to protocol daemon 250 is provided to program 140 (step 645). As will be understood by one of skill in the art, this corresponding password may be identical to that provided to protocol daemon 250, or a mapping technique, such as a hashing algorithm or some other mapping, may be employed to determine correspondence between passwords. Once the password has been provided to program 140 (e.g., a client), program 140 attempts to connect to relay program 210 via firewall 120 using the password (step 650). As illustrated in Fig. 4, relay program 210 attempts to match the password to that of a pre-existing connection listed in its password/connectivity list (step 655).

As with the other connection failures previously described, if the matching process is unsuccessful, related outstanding connections may be terminated (step 620). Alternatively, the connections already appearing as entries in the connectivity list of relay program 210 may simply be allowed to remain, and await further attempts at connection. If a connection having a matching password is found, protocol daemon 250 and relay program 210 begin relaying data between programs 135 and 140 (step 660). This relaying of data continues until one or more of the connections thus formed either fail or are disconnected (step 665) at which time the remaining connections may also be terminated (step 620), although this need not necessarily be the case, as indicated previously.

Fig. 7 is a block diagram illustrating a network architecture 700 according to another embodiment of the present invention. In this embodiment, a server 710 is run on a computer system 720 and is configured to accept only in-bound connections. Computer system 720 is coupled to a network 730 via a firewall 740. Firewall 740 is configured to allow only out-bound connections from computer systems protected thereby (e.g., computer system 720). As noted previously, firewall 740 can protect computer systems such as computer system 720 in a number of ways. For example,



firewall 740 can protect computer system 720 by allowing only out-bound connections (i.e., preventing in-bound connections from network 730). This means that connections can only be created by a protected computer system, and not by outside computer systems, thus preventing access initiated by outside entities.

5 Also coupled to network 730 is a computer system 750 that runs a client 760. As can be seen in Fig. 7, computer system 750 is coupled directly to network 730 (i.e., computer system 750 is not protected by a firewall such as firewall 740). That being the case, client 760 may be configured to receive in-bound connections without the obstacles that a firewall coupled between computer system 750 and network 730  
10 would present. However, assuming server 710 requires an in-bound connection, firewall 740 presents such obstacles to a connection between client 760 and server 710. In order to overcome such obstacles, a protocol daemon 770 is provided on computer system 720.

Protocol daemon 770 initiates an internal connection 780 to server 710, and  
15 also initiates an out-bound connection 790 to client 760. By initiating internal connection 780 to server 710, protocol daemon 770 addresses the need of server 710 for an in-bound (in relative terms) connection. In a similar manner, by initiating out-bound connection 790 to client 760, protocol daemon 770 addresses the restrictions placed on connections by firewall 740. As before, protocol daemon 770 couples  
20 internal connection 780 and out-bound connection 790 allowing the transfer of data through firewall 740 without requiring firewall 740 to admit an in-bound connection. As has been alluded to, the difficulty in initiating a connection through firewall 740 is problematic because of the need of server 710 for an in-bound connection and the preclusion of such connection by firewall 740. The inventors determined that, if  
25 client 760 only supports out-bound connections (i.e., is only capable of initiating connections and not receiving connections), a process such as protocol daemon 770 (or relay program 210) should be provided. Such a process should be provided either on computer system 750 or on a computer system coupled between computer system 750 and firewall 740, so as to be able to receive out-bound connection 790 and couple

that connection to an out-bound connection from client 760 (in the manner depicted in Fig. 2).

Fig. 8 is a flow diagram illustrating a process for data transfer in a network such as that depicted as network architecture 700. As before, the process begins by executing protocol daemon 770 (step 800). Protocol daemon 770 then attempts to create a connection to server 710 (depicted in Fig. 7 as internal connection 780) (step 810). If the creation of internal connection 780 is unsuccessful (step 820), the attempted connection (and optionally any related connections) is terminated (step 830). If internal connection 780 is successfully created, protocol daemon 770 then attempts to create a connection to client 760 (depicted in Fig. 7 as out-bound connection 790) (step 840). If the creation of outbound connection 790 is unsuccessful (step 850), the attempted connection (and any existing related connections) are terminated (step 830), again assuming that the termination of existing connections is desired. If outbound connection 790 is successfully created, protocol daemon 770 then begins relaying data between client 760 and server 710 (step 860). This relaying of data continues until one or both of internal connection 780 and out-bound connection 790 either fail or are disconnected (step 870), at which time any remaining connections may be terminated, if desired (step 830).

While particular embodiments of the present invention have been shown and described, it will be obvious to those skilled in the art that, based upon the teachings herein, changes and modifications may be made without departing from this invention and its broader aspects and, therefore, the appended claims are to encompass within their scope all such changes and modifications as are within the true spirit and scope of this invention. Furthermore, it is to be understood that the invention is solely defined by the appended claims.

**WHAT IS CLAIMED IS:**

1           1.       A method of communicating information between a first program and a  
2 second program over a network comprising:  
3           relaying said information between said first program and a first  
4           communications program over a first network connection;  
5           relaying said information between said first communications program and a  
6           second communications program over a second network connection,  
7           wherein  
8           said first communications program creates said second network  
9           connection to said second communications program through a  
10          first firewall program,  
11          said first firewall program prevents access to said first program  
12          initiated by said second program, and  
13          said second network connection is initiated by said first  
14          communications program; and  
15          relaying said information between said second communications program and  
16          said second program over a third network connection.

1           2.       The method of claim 1, wherein said first program, said first  
2 communications program, said second communications program and said first firewall  
3 program are executed on a first computer system.

1           3.       The method of claim 1, wherein said second communications program  
2 and said second program are executed on a first computer system.

1           4.       The method of claim 1, wherein said first communications program is  
2 a protocol daemon and said second communications program is a relay program.

1           5.       The method of claim 1, wherein said first firewall program also  
2 prevents access to said first program initiated by said second communications  
3 program.

1           6.       The method of claim 1, wherein said first communications program  
2       relays said information between said first and said second network connections.

1           7.       The method of claim 1, wherein said second communications program  
2       relays said information between said second and said third network connections.

1           8.       The method of claim 1, wherein  
2       said first program requires said first network connection to be initiated as an  
3               in-bound network connection relative to said first program,  
4       said first network connection is initiated by said first communications  
5               program, and  
6       said first network connection is in-bound relative to said first program.

1           9.       The method of claim 1, wherein  
2       said first firewall program prevents access to said first program by preventing  
3               an in-bound network connection to said first program, said in-bound  
4               network connection being in-bound relative to said first program, and  
5       said second network connection is created as an out-bound network connection  
6               from said first communications program to said second  
7               communications program.

1           10.      The method of claim 1, wherein  
2       said third network connection is created through a second firewall program,  
3       said second firewall program prevents access to said second program initiated  
4               by said second communications program, and  
5       said third network connection is initiated by said second program.

1           11.      The method of claim 10, wherein said second firewall program  
2       prevents access to said second program by inhibiting an in-bound network connection  
3       to said second program, said in-bound network connection being in-bound relative to  
4       said second program.

1           12.    A method of communicating information between a first program and a  
2 second program over a network comprising:  
3           relaying said information between said first program and a first  
4           communications program over a first network connection, wherein  
5           said first program creates said first network connection to said first  
6           communications program through a first firewall program,  
7           said first firewall program prevents access to said first program  
8           initiated by said second program, and  
9           said first network connection is initiated by said first program; and  
10          relaying said information between said first communications program and said  
11          second program over a second network connection.

1           13.    The method of claim 12, wherein said first program, said first  
2 communications program and said first firewall program are executed on a first  
3 computer system.

1           14.    The method of claim 12, wherein said first communications program is  
2 a relay program.

1           15.    The method of claim 12, wherein said first firewall program also  
2 prevents access to said first program initiated by said first communications program.

1           16.    The method of claim 12, wherein  
2 said first firewall program prevents access to said first program by preventing  
3 an in-bound network connection to said first program, said in-bound  
4 network connection being in-bound relative to said first program, and  
5 said first network connection is created as an out-bound network connection  
6 from said first program to said first communications program.

1           17.    The method of claim 12, wherein.  
2           said second network connection is created from said second program to said  
3           first communications program through a second firewall program,  
4           said second firewall program prevents access to said second program initiated  
5           by said first communications program, and  
6           said second network connection is initiated by said second program.

1           18.    The method of claim 17, wherein said second firewall program  
2           prevents access to said second program by inhibiting an in-bound network connection  
3           to said second program, said in-bound network connection being in-bound relative to  
4           said second program.

1           19.    A method of communicating information over a network comprising:  
2           relaying said information between a first program and a first communications  
3           program over a first network connection, wherein  
4           said first program requires said first network connection to be initiated  
5           as an in-bound network connection relative to said first  
6           program,  
7           said first network connection is initiated by said first communications  
8           program, and  
9           said first network connection is in-bound relative to said first program;  
10          and  
11          relaying said information between said first communications program and a  
12          second program over a second network connection, wherein  
13          said first communications program creates said second network  
14          connection to said second program through a first firewall  
15          program,  
16          said first firewall program prevents access to said first program  
17          initiated by said second program, and  
18          said second network connection is initiated by said first  
19          communications program.

1           20.    The method of claim 19, wherein said first program, said first  
2   communications program and said first firewall program are executed on a first  
3   computer system.

1           21.    The method of claim 19, wherein said first communications program is  
2   a protocol daemon.

1           22.    The method of claim 19, wherein  
2   said first firewall program prevents access to said first program by preventing  
3                said in-bound network connection to be initiated from a side of said  
4                first firewall program that is opposite to a side of said first firewall  
5                program to which said first program is coupled, and  
6   said second network connection is created as an out-bound network connection  
7                from said first communications program to said second program.

1           23.    A method of supporting network communications comprising:  
2                creating a first network connection between a first communications program  
3                and a first program;  
4                creating a second network connection from said first communications program  
5                to a second communications program, wherein said first  
6                communications program creates said second network connection  
7                through a first firewall program;  
8                creating a third network connection between a second program and said  
9                second communications program; and  
10              communicating information between said first program and said second  
11              program by  
12              communicating said information over said first network connection,  
13              said second network connection and said third network  
14              connection,

15 communicating said information between said first network connection  
16 and said second network connection via said first  
17 communications program, and  
18 communicating said information between said second network  
19 connection and said third network connection via said second  
20 communications program.

1 24. The method of claim 23, wherein said first program, said first  
2 communications program, said second communications program and said first firewall  
3 program are executed on a first computer system.

1 25. The method of claim 23, wherein said second communications  
2 program and said second program are executed on a first computer system.

1 26. The method of claim 23, wherein said first communications program is  
2 a protocol daemon and said second communications program is a relay program.

1 27. The method of claim 23, wherein said first firewall program protects  
2 said first program by preventing an in-bound network connection to said first  
3 program, said in-bound network connection being in-bound relative to said first  
4 program.

1 28. The method of claim 23, wherein said third network connection is  
2 created from said second program to said second communications program through a  
3 second firewall program, wherein said second firewall program prevents an in-bound  
4 network connection to said second program, said in-bound network connection being  
5 in-bound relative to said second program.

1 29. The method of claim 23, further comprising:  
2 providing a first instance of a password to said first communications program;



3 passing said first instance of said password from said first communications  
 4 program to said second communications program during creation of  
 5 said second network connection;  
 6 providing a second instance of said password to said second program;  
 7 passing said second instance of said password from said second program to  
 8 said second communications program during creation of said third  
 9 network connection; and  
 10 associating said second connection with said third connection using said first  
 11 and said second instances of said password.

1 30. The method of claim 29, wherein said passing said first instance of said  
 2 password further comprises:  
 3 sending said first instance of said password from said first communications  
 4 program to said second communications program; and  
 5 entering information regarding said second network connection and said  
 6 password in a connection list maintained by said second  
 7 communications program, said first instance of said password being  
 8 entered in a password entry.

1 31. The method of claim 29, wherein said associating further comprises:  
 2 matching said second instance of said password with said password entry in  
 3 said connection list, said password entry containing said password;  
 4 entering information regarding said third network connection in said  
 5 connection list; and  
 6 associating said second and third connections.

1 32. The method of claim 31, wherein said associating said second and third  
 2 connections further comprises:  
 3 relaying said information between said second and third connections.

1           33.    A computer program product encoded in computer readable media for  
2 relaying information between a first program and a second program over a network,  
3 the computer program product comprising:  
4           a first set of instructions, executable by a processor and configured to cause  
5           said processor to relay said information between said first program and  
6           a first communications program over a first network connection;  
7           a second set of instructions, executable by said processor and configured to  
8           cause said processor to relay said information between said first  
9           communications program and a second communications program over  
10          a second network connection, wherein  
11          said first communications program creates said second network  
12          connection to said second communications program through a  
13          first firewall program,  
14          said first firewall program prevents access to said first program  
15          initiated by said second program, and  
16          said second network connection is initiated by said first  
17          communications program; and  
18          a third set of instructions, executable by said processor and configured to  
19          cause said processor to relay said information between said second  
20          communications program and said second program over a third  
21          network connection.

1           34.    The computer program product of claim 33, wherein said first set of  
2 instructions and said second set of instructions are executed on a first computer  
3 system.

1           35.    The computer program product of claim 33, wherein said first firewall  
2 program also prevents access to said first program initiated by said second  
3 communications program.

1           36.     The computer program product of claim 33, wherein said first program  
2 is executed on a first processor, said first communications program is executed on a  
3 second processor, said second communications program is executed on a third  
4 processor and said second program is executed on a fourth processor.

1           37.     The computer program product of claim 33, wherein said first program  
2 is executed on a first processor, first communications program is executed on a  
3 second processor and said second program is executed on a third processor.

1           38.     The computer program product of claim 33, wherein  
2 said first program requires said first network connection to be initiated as an  
3 in-bound network connection relative to said first program,  
4 said first network connection is initiated by said first communications  
5 program, and  
6 said first network connection is in-bound relative to said first program.

1           39.     The computer program product of claim 33, wherein  
2 said first firewall program prevents access to said first program by preventing  
3 an in-bound network connection to said first program, said in-bound  
4 network connection being in-bound relative to said first program, and  
5 said second network connection is created as an out-bound network connection  
6 from said first communications program to said second  
7 communications program.

1           40.     The computer program product of claim 33, wherein  
2 said third network connection is created through a second firewall program,  
3 said second firewall program prevents access to said second program initiated  
4 by said second communications program, and  
5 said third network connection is initiated by said second program.

1           41.     The computer program product of claim 40, wherein said second  
2     firewall program prevents access to said second program by inhibiting an in-bound  
3     network connection to said second program, said in-bound network connection being  
4     in-bound relative to said second program.

1           42.     A computer program product encoded in computer readable media for  
2     communicating information over a network, the computer program product  
3     comprising:

4                 a first set of instructions, executable by a processor and configured to cause  
5                         said processor to relay said information between a first program and a  
6                         first communications program over a first network connection by  
7                         virtue of being configured to cause said processor to create said first  
8                         network connection from said first program to said first  
9                         communications program through a first firewall program, wherein  
10                        said first firewall program prevents access to said first program  
11                        initiated by a second program, and  
12                        said first network connection is initiated by said first program; and  
13                 a second set of instructions, executable on said processor and configured to  
14                         cause said processor to relay said information between said first  
15                         communications program and said second program over a second  
16                         network connection.

1           43.     The computer program product of claim 42, wherein said first set of  
2     instructions and said second set of instructions are executed on a first computer  
3     system.

1           44.     The computer program product of claim 42, wherein said first program  
2     is executed on a first processor, said first communications program is executed on a  
3     second processor and said second program is executed on a third processor.

1           45.     The computer program product of claim 42, wherein said first firewall  
2     program also prevents access to said first program initiated by said first  
3     communications program.

1           46.     The computer program product of claim 42, wherein said first  
2     communications program is a relay program.

1           47.     The computer program product of claim 42, further comprising:  
2     a third set of instructions, executable on said processor and configured to  
3                 cause said processor to prevent access to said first program through  
4                 said first firewall program by virtue of being configured to prevent an  
5                 in-bound network connection to said first program, said in-bound  
6                 network connection being in-bound relative to said first program, and  
7     a fourth set of instructions, executable on said processor and configured to  
8                 cause said processor to create said first network connection as an out-  
9                 bound network connection from said first program to said first  
10     communications program.

1           48.     The computer program product of claim 42, further comprising:  
2     a third set of instructions, executable on said processor and configured to  
3                 cause said processor to create said second network connection from  
4                 said second program to said first communications program through a  
5                 second firewall program;  
6     a fourth set of instructions, executable on said processor and configured to  
7                 cause said processor to prevent access to said second program initiated  
8                 by said first communications program through said second firewall  
9                 program; and  
10     a fifth set of instructions, executable on said processor and configured to cause  
11                 said processor to initiate said second network connection from said  
12     second program.

1           49.     The computer program product of claim 42, further comprising:  
 2           a sixth set of instructions, executable on said processor and configured to  
 3           cause said processor to prevent access to said second program through  
 4           said second firewall program by inhibiting an in-bound network  
 5           connection to said second program, said in-bound network connection  
 6           being in-bound relative to said second program;

1           50.     A computer program product encoded in computer readable media for  
 2     communicating information between a first program and a second program over a  
 3     network, the computer program product comprising:  
 4           a first set of instructions, executable by a processor and configured to cause  
 5           said processor to relay said information between a first program and a  
 6           first communications program over a first network connection, wherein  
 7           said first program requires said first network connection to be initiated  
 8           as an in-bound network connection relative to said first  
 9           program,  
 10          said first network connection is initiated by said first communications  
 11          program, and  
 12          said first network connection is in-bound relative to said first program;  
 13          and  
 14          a second set of instructions, executable on said processor and configured to  
 15          cause said processor to relay said information between said first  
 16          communications program and a second program over a second network  
 17          connection, wherein  
 18          said first communications program creates said second network  
 19          connection to said second program through a first firewall  
 20          program,  
 21          said first firewall program prevents access to said first program  
 22          initiated by said second program, and  
 23          said second network connection is initiated by said first  
 24          communications program.

1           51.     The computer program product of claim 50, wherein said first set of  
2 instructions and said second set of instructions are executed on a first computer  
3 system.

1           52.     The computer program product of claim 50, wherein said first  
2 communications program is a protocol daemon.

1           53.     The computer program product of claim 52, wherein said plurality of  
2 entries comprises a routing table, further comprising:  
3           a third set of instructions, executable on said processor and configured to  
4           cause said processor to prevent access to said first program by virtue of  
5           said first firewall program preventing said in-bound network  
6           connection to be initiated from a side of said first firewall program that  
7           is opposite to a side of said first firewall program to which said first  
8           program is coupled; and  
9           a fourth set of instructions, executable on said processor and configured to  
10          cause said processor to create said second network connection as an  
11          out-bound network connection from said first communications  
12          program to said second program.

1           54.     A network comprising:  
2           a first program executed on a first computer;  
3           a first firewall program executed on a second computer coupled to said first  
4           computer;  
5           a second program executed on a third computer coupled to said second  
6           computer; and  
7           a third program executed on a fourth computer coupled to said third computer,  
8           wherein  
9           said first firewall program is configured to prevent access to said first  
10          program initiated by said third program,





09136632 120999

1           61.     The network of claim 57, wherein  
2           said first firewall program is configured to prevent access to said first program  
3           by virtue of being configured to prevent an in-bound network  
4           connection to said first program, said in-bound network connection  
5           being in-bound relative to said first program, and  
6           said first program is configured to create said first network connection as an  
7           out-bound network connection from said first program to said second  
8           program.

1           62.     The network of claim 57, wherein.  
2           said second network connection is created from said second program to said  
3           first communications program through a second firewall program,  
4           said second firewall program prevents access to said second program initiated  
5           by said first communications program, and  
6           said second network connection is initiated by said second program.

1           63.     The network of claim 54, further comprising:  
2           a fourth program executed on a fifth computer coupled to said first computer,  
3           wherein  
4           said first program is configured to initiate a third network connection  
5           to said fourth program, said third network connection being in-  
6           bound relative to said fourth program, and  
7           said fourth program is configured to require said third network  
8           connection to be initiated as an in-bound network connection  
9           relative to said fourth program.

1           64.     The network of claim 63, wherein said first firewall program also  
2           prevents access to said first program initiated by said second program.

1           65.     The network of claim 63, wherein said first firewall program also  
2           prevents access to said fourth program initiated by said second program.

1        66.    The network of claim 63, wherein  
 2        said first firewall program prevents access to said first and said fourth  
 3                programs by preventing in-bound network connections to said first and  
 4                said fourth programs, and  
 5        said first network connection is created as an out-bound network connection  
 6                from said first program to said second program.

1        67.    The network of claim 63, wherein  
 2        said third network connection is created through a second firewall program,  
 3        said second firewall program prevents access to said third program initiated by  
 4                said first and said second programs, and  
 5        said third network connection is initiated by said third program.

1        68.    The network of claim 63, wherein said second firewall program  
 2        prevents access to said third program by inhibiting an in-bound network connection to  
 3        said third program, said in-bound network connection being in-bound relative to said  
 4        third program.

1        69.    A network comprising:  
 2                a first program executed on a first computer;  
 3                a second program executed on a second computer coupled to said first  
 4                computer;  
 5                a first firewall program executed on a third computer coupled to said first  
 6                computer;  
 7                a third program executed on a fourth computer coupled to said second  
 8                computer, wherein  
 9                said first firewall program is configured to prevent access to said first  
 10                program initiated by said third program,  
 11                said first program is configured to initiate a first network connection to  
 12                said second program through said first firewall program,

13                   said second program is configured to initiate a second network  
14                   connection to said first program, said second network  
15                   connection being in-bound relative to said first program, and  
16                   said first program is configured to require said second network  
17                   connection to be initiated as an in-bound network connection  
18                   relative to said first program.

1           70.    The network of claim 69, wherein said first program, said second  
2   program and said first firewall program are executed on said first computer.

1           71.    The network of claim 69, wherein  
2   said first firewall program prevents access to said first program by preventing  
3                   said in-bound network connection to be initiated from a side of said  
4                   first firewall program that is opposite to a side of said first firewall  
5                   program to which said first program is coupled, and  
6   said second network connection is created as an out-bound network connection  
7                   from said second program to said third program.

1           72.    The network of claim 71, wherein said first firewall program is also  
2   configured to prevent access to said second program initiated by said third program.

1           73.    A method of communicating information between a first program and a  
2   second program over a network comprising:  
3                   creating a first out-bound network connection from a first communications  
4                   program to said first program, wherein said first out-bound network  
5                   connection is out-bound relative to said first communications program;  
6                   creating a second out-bound network connection from said first  
7                   communications program to said second program through a first  
8                   firewall program, wherein  
9                   said second out-bound network connection is out-bound relative to said  
10                   first communications program

563025 v2  
Client Reference: 51021 Weil #1669

11           said first firewall program prevents in-bound access to said first  
 12           program,  
 13           said in-bound access is a network connection that is in-bound relative  
 14           to said first program, and  
 15           said first program is configured to accept only an in-bound connection  
 16           to said first program; and  
 17           relaying said information between said first out-bound network connection and  
 18           said second out-bound network connection, said relaying performed by  
 19           said first communications program.

1           74.    The method of claim 73, wherein said first communications program is  
 2           a protocol daemon.

1           75.    The method of claim 73, wherein said second out-bound network  
 2           connection is created through a second firewall program, wherein said second firewall  
 3           program prevents in-bound access to said second program.

1           76.    The method of claim 73, wherein said first program, said first  
 2           communications program and said first firewall program are executed on a first  
 3           computer system.

1           77.    A computer system comprising:  
 2           a processor;  
 3           computer readable medium coupled to said processor; and  
 4           computer code, encoded in said computer readable medium, configured to  
 5           cause said processor to:  
 6           create a first out-bound network connection from a first  
 7           communications program to said first program, wherein said  
 8           first out-bound network connection is out-bound relative to said  
 9           first communications program;

10 create a second out-bound network connection from said first  
 11 communications program to said second program through a  
 12 first firewall program, wherein  
 13 said second out-bound network connection is out-bound  
 14 relative to said first communications program  
 15 said first firewall program prevents in-bound access to said first  
 16 program,  
 17 said in-bound access is a network connection that is in-bound  
 18 relative to said first program, and  
 19 said first program is configured to accept only an in-bound  
 20 connection to said first program; and  
 21 relay said information between said first out-bound network connection  
 22 and said second out-bound network connection, said relaying  
 23 performed by said first communications program.

1 78. The computer system of claim 77, wherein said first communications  
 2 program is a protocol daemon.

1 79. The computer system of claim 77, wherein said computer code  
 2 configured to cause said processor to create said second out-bound network  
 3 connection is further configured to cause said processor to:  
 4 create said second out-bound network connection through a second firewall  
 5 program, wherein said second firewall program prevents in-bound  
 6 access to said second program.

1 80. The computer system of claim 77, wherein said computer code  
 2 configured to cause said processor to create said first out-bound network connection,  
 3 create said second out-bound network connection, and relay said information is  
 4 executed on a single processor.

1           81. A computer program product encoded in computer readable media,  
2 said computer program product comprising:  
3           a first set of instructions, executable on a computer system, configured to  
4           create a first out-bound network connection from a first  
5           communications program to said first program, wherein said first out-  
6           bound network connection is out-bound relative to said first  
7           communications program;  
8           a second set of instructions, executable on said computer system, configured to  
9           create a second out-bound network connection from said first  
10          communications program to said second program through a first  
11          firewall program, wherein  
12          said second out-bound network connection is out-bound relative to said  
13          first communications program  
14          said first firewall program prevents in-bound access to said first  
15          program,  
16          said in-bound access is a network connection that is in-bound relative  
17          to said first program, and  
18          said first program is configured to accept only an in-bound connection  
19          to said first program; and  
20          a third set of instructions, executable on said computer system, configured to  
21          relay said information between said first out-bound network connection  
22          and said second out-bound network connection, said relaying  
23          performed by said first communications program.

1           82. The computer program product of claim 81, wherein said first  
2 communications program is a protocol daemon.

1           83. The computer program product of claim 81, wherein said second set of  
2 instructions comprises:

3           a fourth set of instructions, executable on said computer system, configured to  
4           create said second out-bound network connection through a second

5 firewall program, wherein said second firewall program prevents in-  
6 bound access to said second program.

1 84. The computer program product of claim 81, wherein said first, said  
2 second and said third sets of instructions are executed on a single computer system.

1 85. A method of communicating information between a first program and a  
2 second program over a network comprising:

3 creating a first out-bound network connection from said first program to a first  
4 communications program through a first firewall program, wherein  
5 said first out-bound network connection is out-bound relative to said  
6 first program, and  
7 said first firewall program prevents in-bound access to said first  
8 program; and  
9 creating a second out-bound network connection from said second program to  
10 said first communications program through a second firewall program,  
11 wherein  
12 said second out-bound network connection is out-bound relative to said  
13 second program, and  
14 said second firewall program prevents in-bound access to said second  
15 program; and  
16 relaying said information between said first out-bound network connection and  
17 said second out-bound network connection, said relaying performed by  
18 said first communications program.

1 86. The method of claim 85, wherein said first communications program is  
2 a relay program.

1 87. The method of claim 85, further comprising:  
2 creating a third out-bound network connection from said first program to a  
3 third program.

1           88.     The method of claim 87, wherein  
2           said third out-bound network connection is out-bound relative to said first  
3           program and in-bound relative to said third program, and  
4           said third program is configured to accept only an in-bound connection to said  
5           third program.

1           89.     The method of claim 85, wherein said first program, said first  
2           communications program and said first firewall program are executed on a first  
3           computer system.

1           90.     The method of claim 85, wherein said second program, said first  
2           communications program and said second firewall program are executed on a first  
3           computer system.

1           91.     A computer system comprising:  
2           a processor;  
3           computer readable medium coupled to said processor; and  
4           computer code, encoded in said computer readable medium, configured to  
5           cause said processor to:  
6           create a first out-bound network connection from said first program to  
7           a first communications program through a first firewall  
8           program, wherein  
9           said first out-bound network connection is out-bound relative to  
10          said first program, and  
11          said first firewall program prevents in-bound access to said first  
12          program; and  
13          create a second out-bound network connection from said second  
14          program to said first communications program through a  
15          second firewall program, wherein  
16          said second out-bound network connection is out-bound  
17          relative to said second program, and

09456632 123959



18                   said second firewall program prevents in-bound access to said  
19                   second program; and  
20                   relay said information between said first out-bound network connection  
21                   and said second out-bound network connection, said relaying  
22                   performed by said first communications program.

1           92.    The computer system of claim 91, wherein said first communications  
2   program is a relay program.

1           93.    The computer system of claim 91, wherein said computer code is  
2   further configured to cause said processor to:  
3           create a third out-bound network connection from said first program to a third  
4           program.

1           94.    The computer system of claim 93, wherein  
2   said third out-bound network connection is out-bound relative to said first  
3           program and in-bound relative to said third program, and  
4   said third program is configured to accept only an in-bound connection to said  
5           third program.

1           95.    The computer system of claim 91, wherein said first program, said first  
2   communications program and said first firewall program are executed on a single  
3   processor.

1           96.    The computer system of claim 91, wherein said second program, said  
2   first communications program and said second firewall program are executed on a  
3   first computer system.

1           97.    A computer program product encoded in computer readable media,  
2   said computer program product comprising:  
3           a first set of instructions, executable on a computer system, configured to  
4           create a first out-bound network connection from said first program to

5 a first communications program through a first firewall program,  
6 wherein  
7 said first out-bound network connection is out-bound relative to said  
8 first program, and  
9 said first firewall program prevents in-bound access to said first  
10 program; and  
11 a second set of instructions, executable on said computer system, configured to  
12 create a second out-bound network connection from said second  
13 program to said first communications program through a second  
14 firewall program, wherein  
15 said second out-bound network connection is out-bound relative to said  
16 second program, and  
17 said second firewall program prevents in-bound access to said second  
18 program; and  
19 a third set of instructions, executable on said computer system, configured to  
20 relay said information between said first out-bound network connection  
21 and said second out-bound network connection, said relaying  
22 performed by said first communications program.

1 98. The computer program product of claim 97, wherein said first  
2 communications program is a relay program.

1 99. The computer program product of claim 97, wherein said computer  
2 program product further comprises:  
3 a fourth set of instructions, executable on said computer system, configured to  
4 create a third out-bound network connection from said first program to  
5 a third program.

1 100. The computer program product of claim 99, wherein  
2 said third out-bound network connection is out-bound relative to said first  
3 program and in-bound relative to said third program, and

0343693 120999

4           said third program is configured to accept only an in-bound connection to said  
5           third program.

1           101.   The computer program product of claim 97, wherein said first program,  
2   said first communications program and said first firewall program are executed on a  
3   single processor.

1           102.   The computer program product of claim 97, wherein said second  
2   program, said first communications program and said second firewall program are  
3   executed on a first computer system.

## METHOD AND APPARATUS SUPPORTING NETWORK COMMUNICATIONS THROUGH A FIREWALL

Fry, Steven G.  
Sarkar, Shantanu

### 5    ABSTRACT

          A method of communicating information between a first program and a  
second program over a network is described. The method includes relaying the  
information between the first program and a first communications program over a first  
network connection, relaying the information between the first communications  
10    program and a second communications program over a second network connection  
and relaying the information between the second communications program and the  
second program over a third network connection. Further, the first communications  
program creates the second network connection to the second communications  
15    program through a first firewall program, which prevents access to the first program  
initiated by the second program. Thus, the second network connection is initiated by  
the first communications program. As will be discussed, the first communications  
program can be, for example, a protocol daemon and the second communications  
program can be, for example, a relay program. The first firewall program can also be  
20    configured to prevent access to the first program initiated by the second  
communications program.

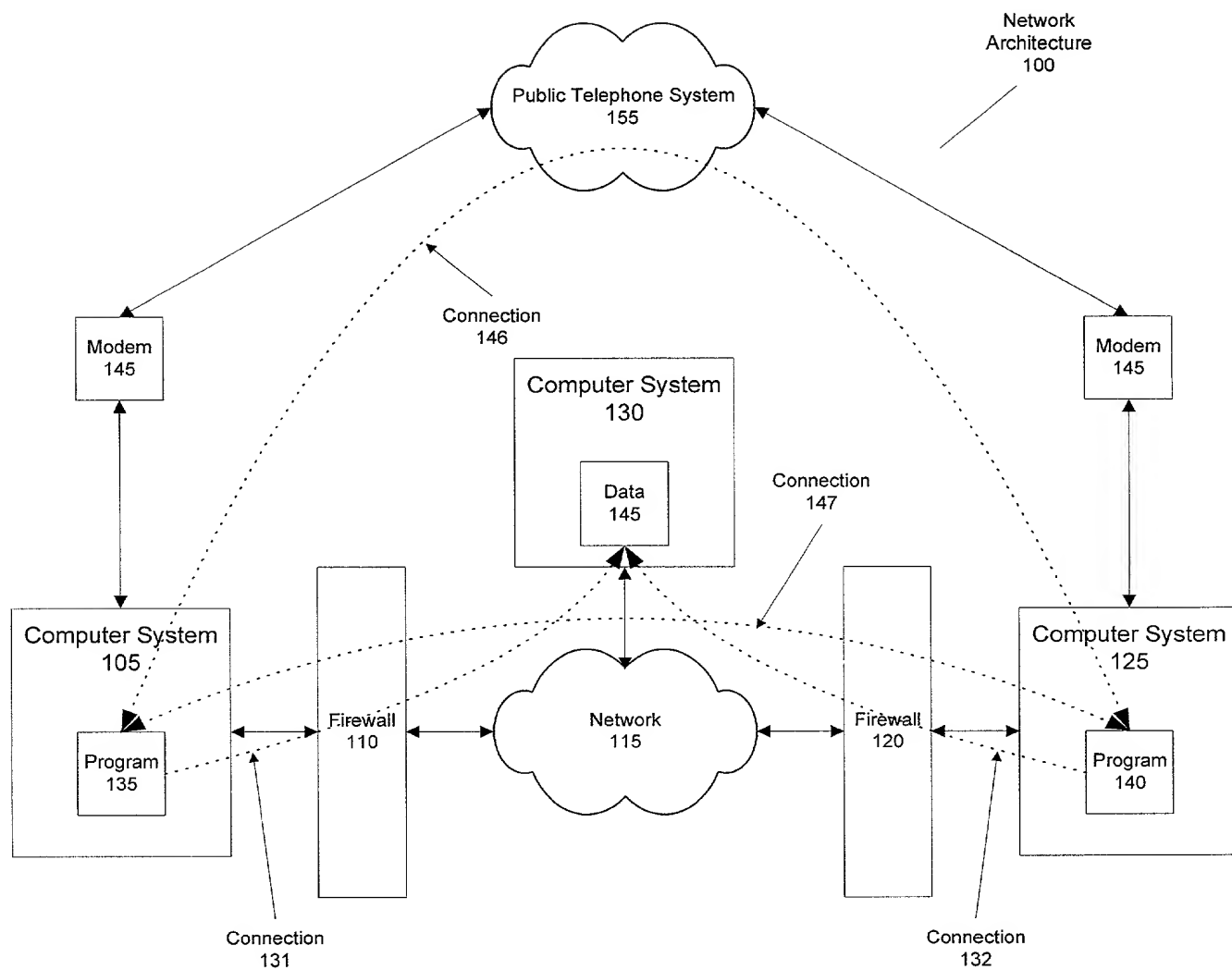


Fig. 1  
(Prior Art)

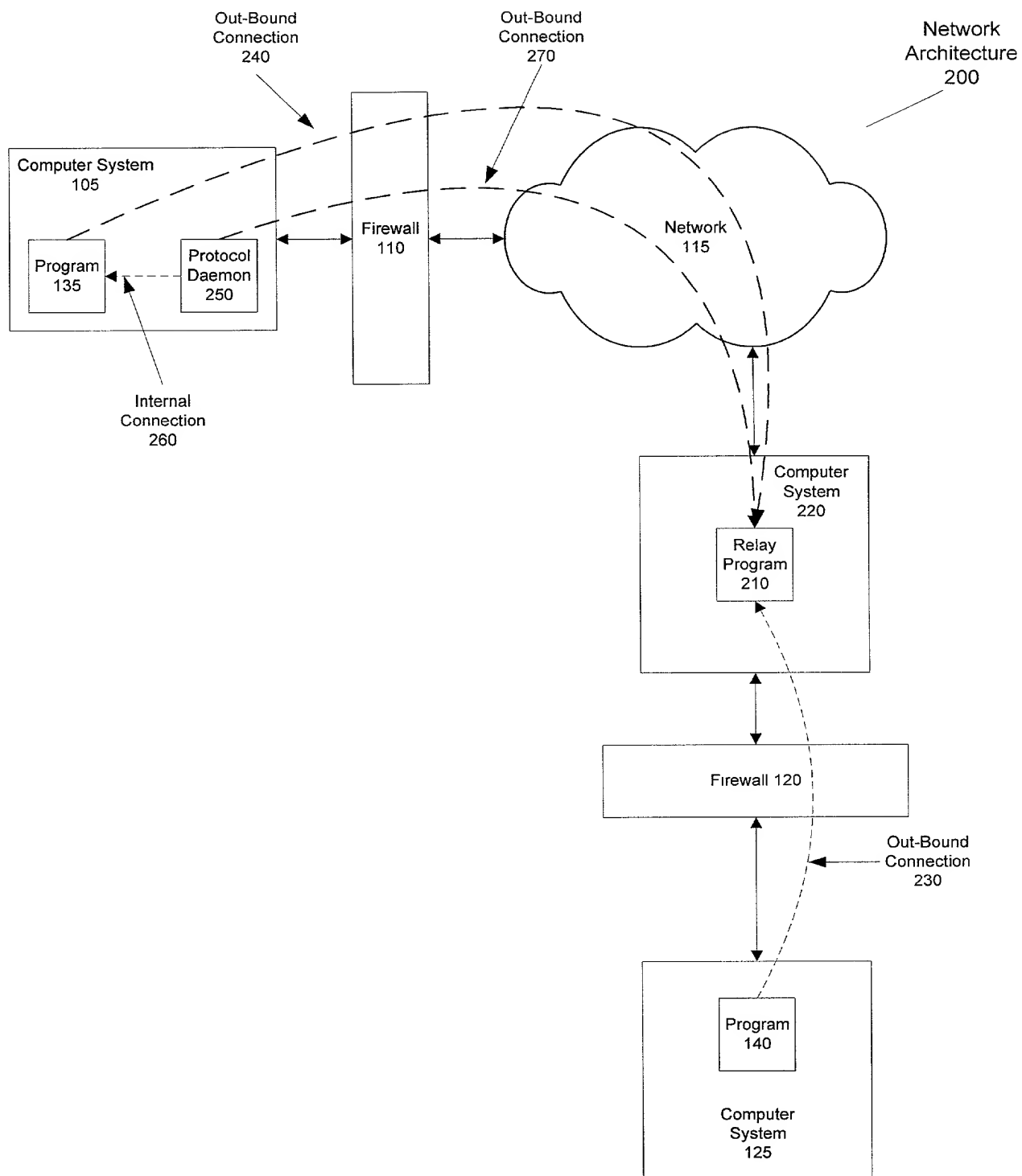


Fig. 2

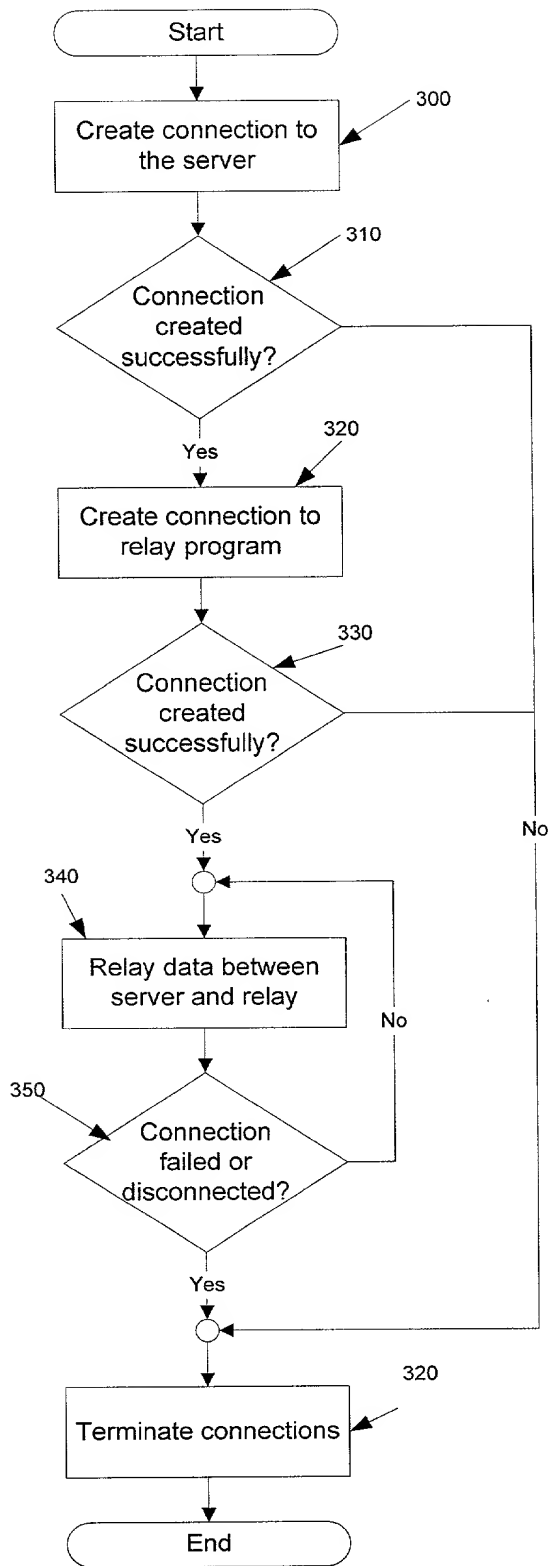


Fig. 3

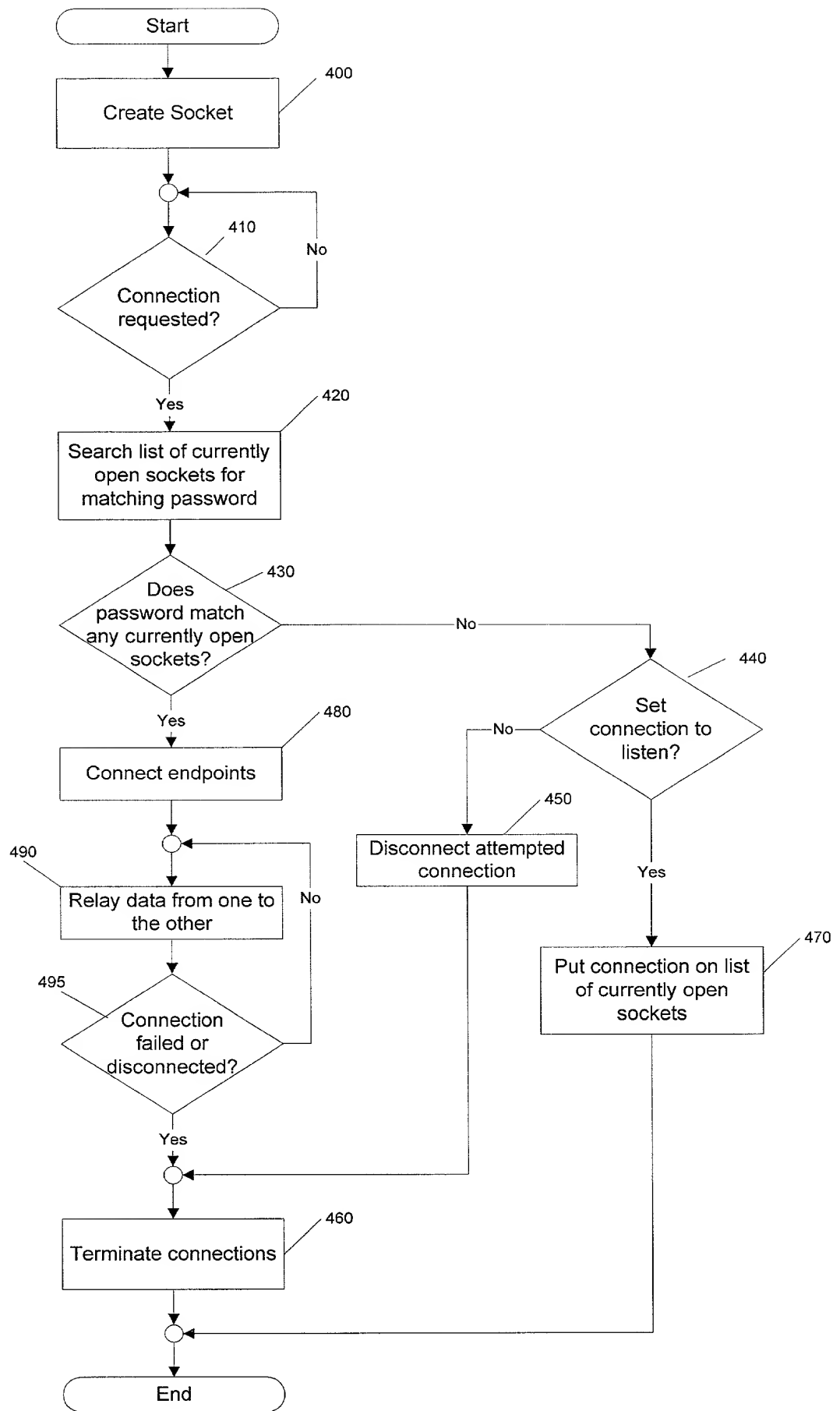


Fig. 4



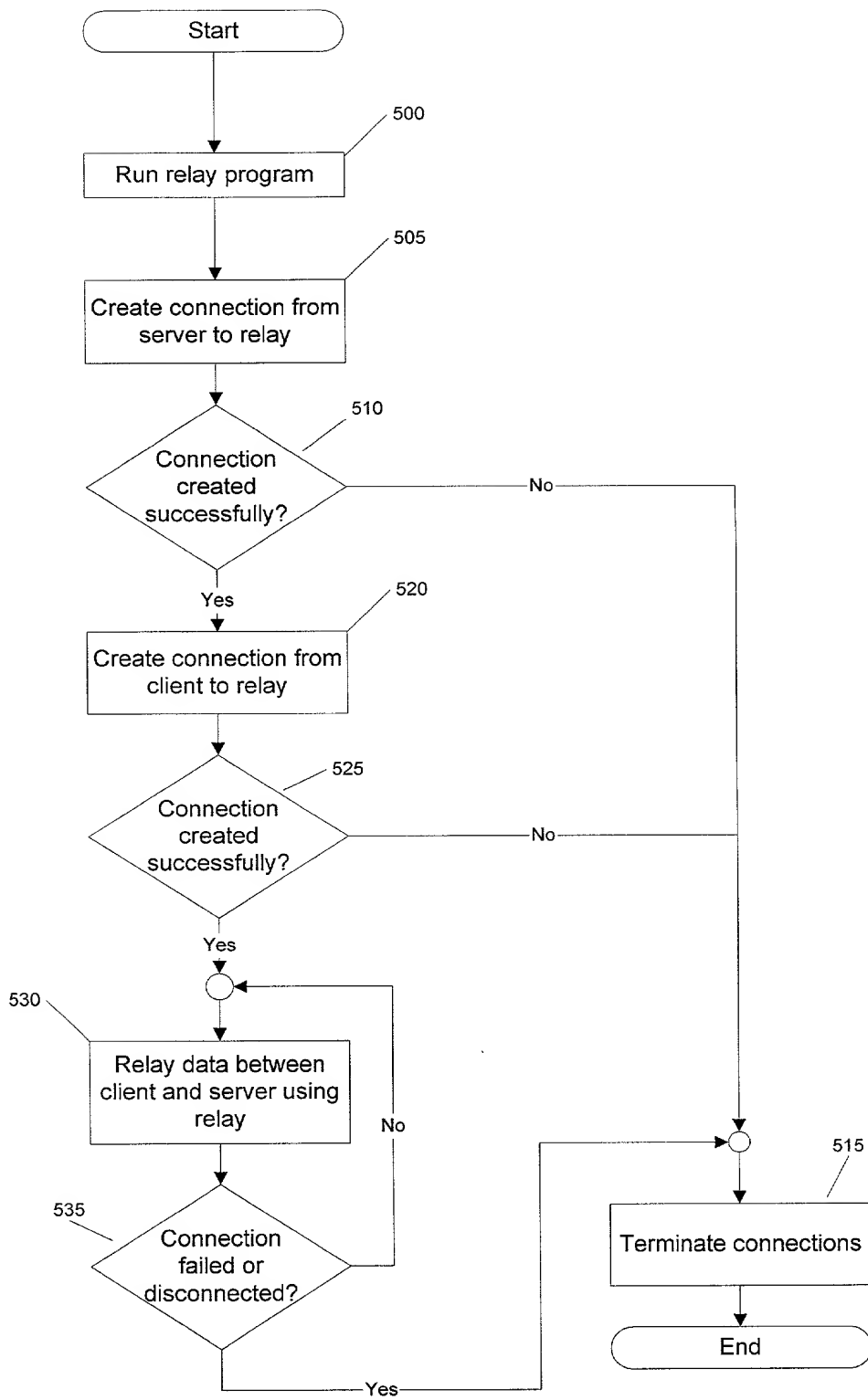
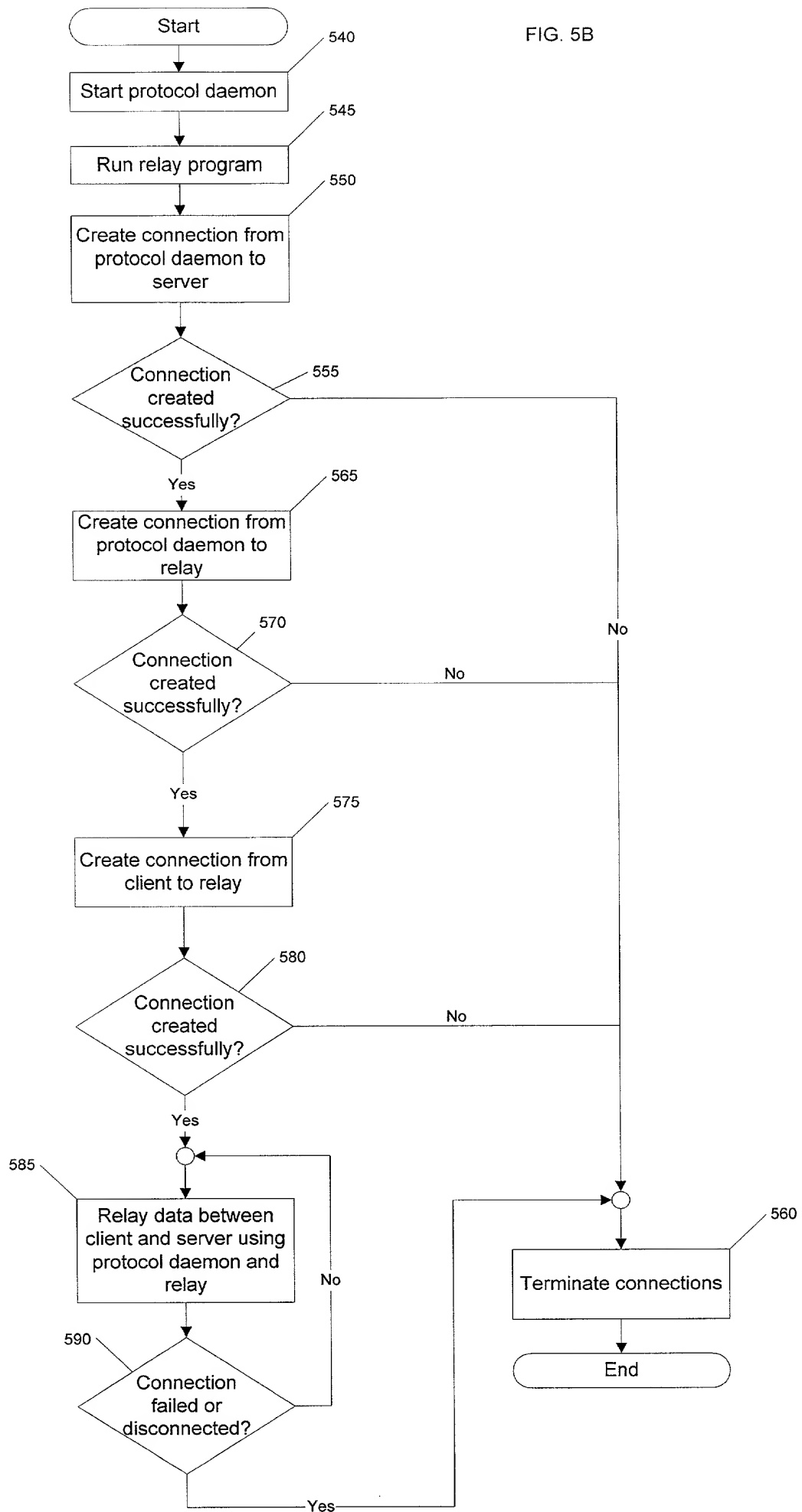


Fig. 5A



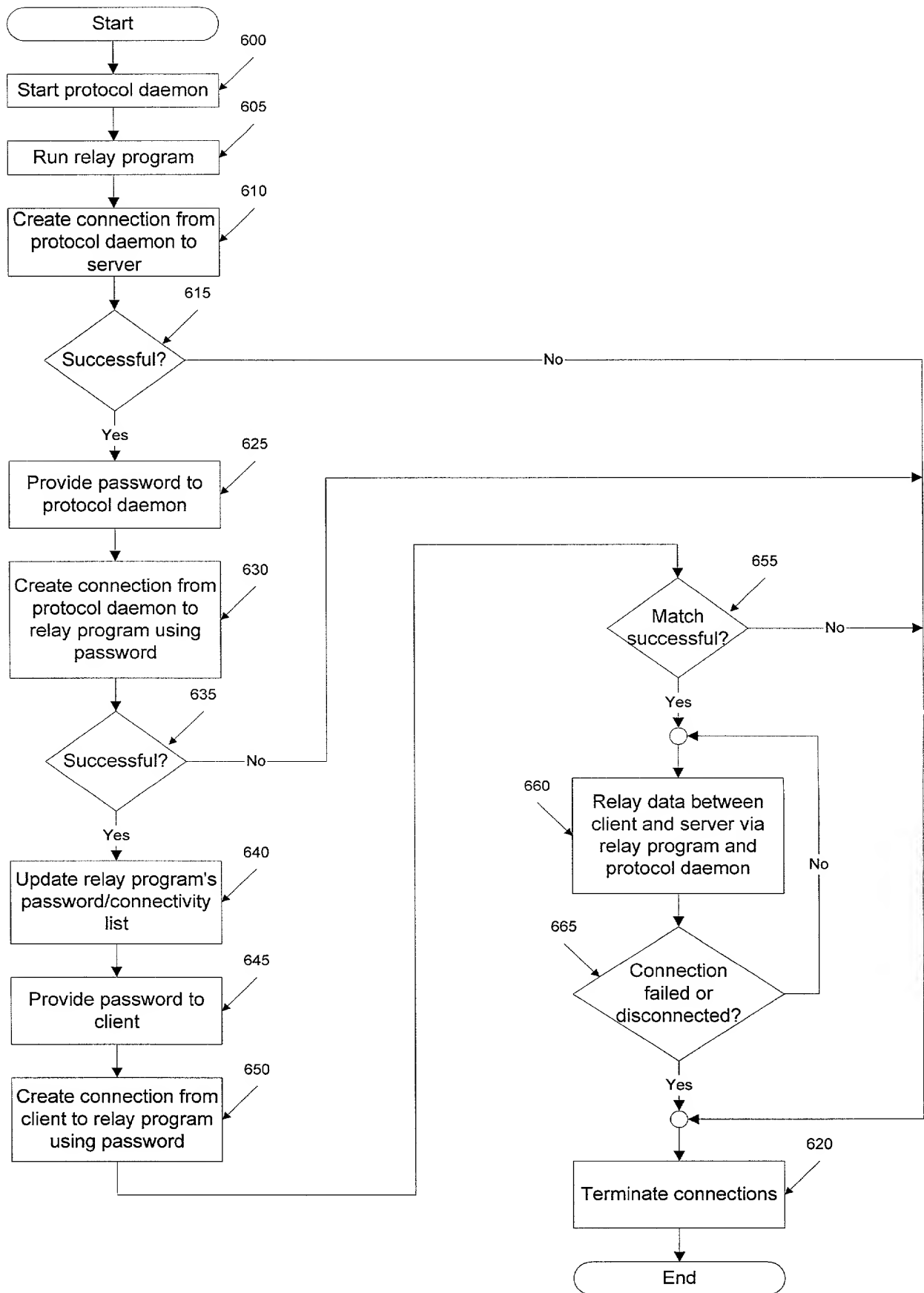


Fig. 6

00436536 100909

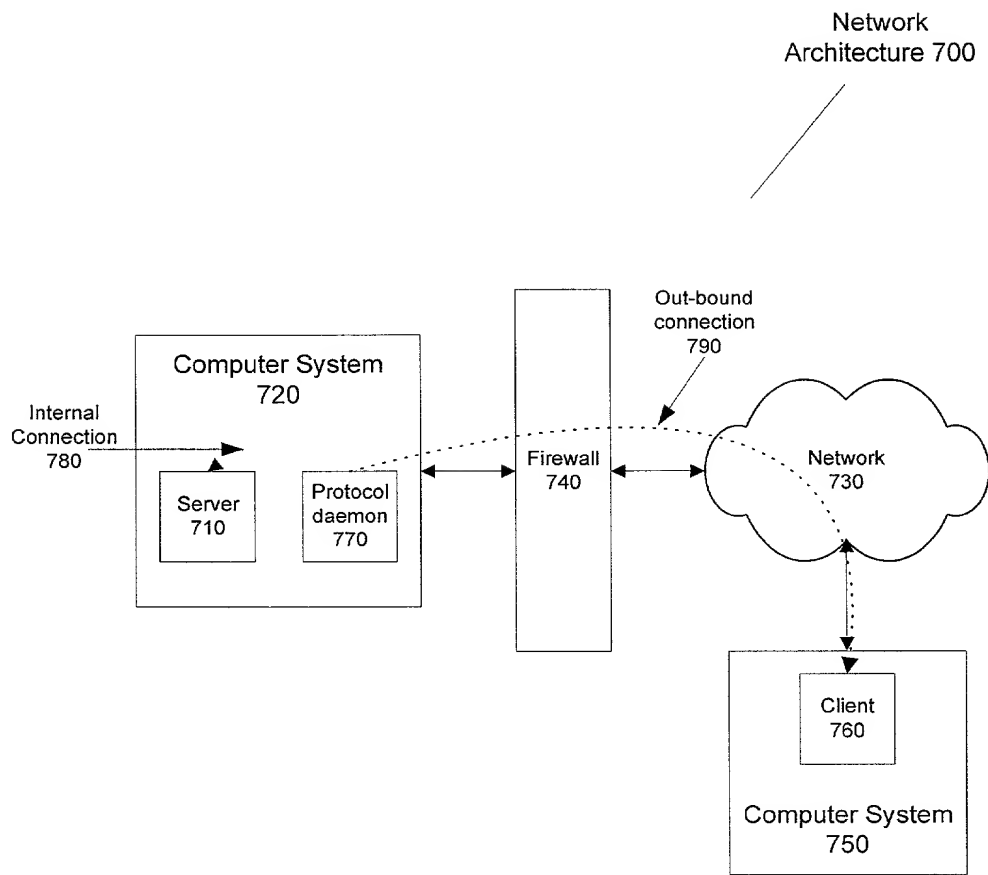


Fig. 7

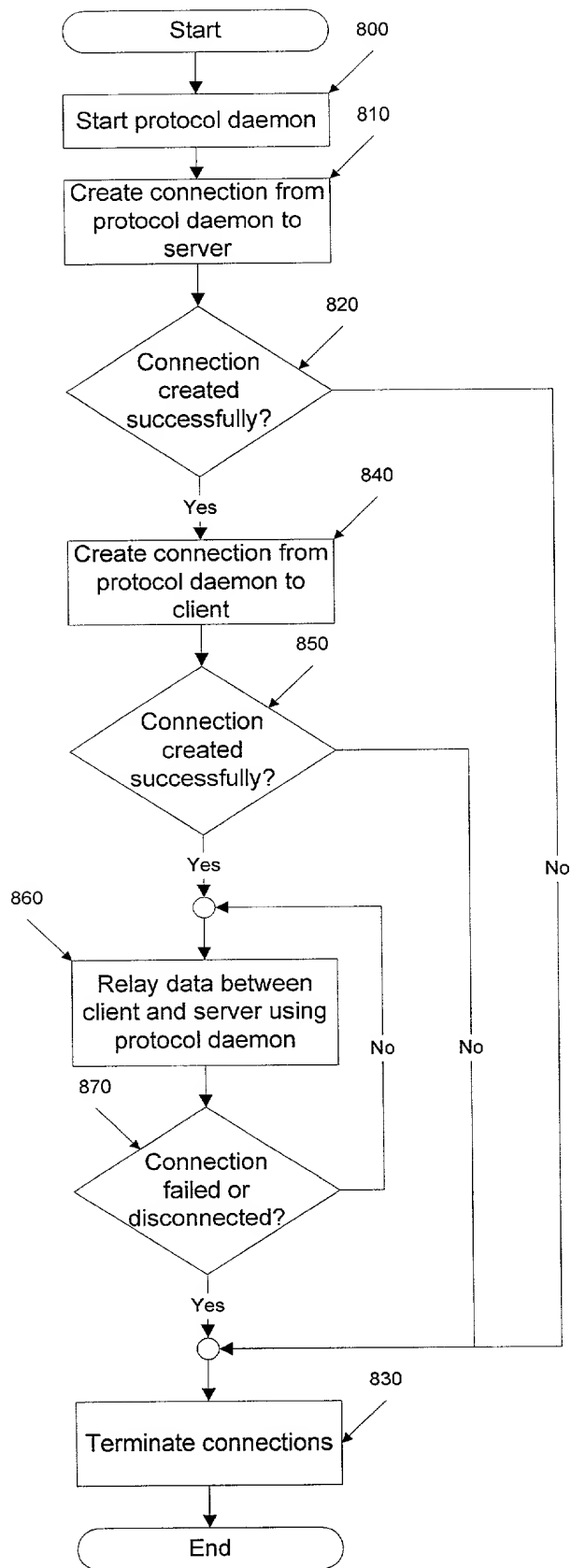


Fig. 8

# DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below adjacent to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of subject matter (process, machine, manufacture, or composition of matter, or an improvement thereof) which is claimed and for which a patent is sought by way of the application entitled

## Method And Apparatus Supporting Network Communications Through A Firewall

which (check) ☒ is attached hereto.

☐ and is amended by the Preliminary Amendment attached hereto.

☐ was filed on \_\_\_\_\_ as Application Serial No. \_\_\_\_\_

☐ and was amended on \_\_\_\_ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
Number	Country	Day/Month/Year Filed	Yes	No
N/A			<input type="checkbox"/>	<input type="checkbox"/>

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

Provisional Application Number	Filing Date
N/A	

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or PCT international application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status (patented, pending, abandoned)
N/A		

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith:

Alan H. MacPherson (24,423); Brian D. Ogonowsky (31,988); David W. Heid (25,875); Norman R. Klivans (33,003); Edward C. Kwok (33,938); David E. Steuber (25,557); Michael Shenker (34,250); Stephen A. Terrile (32,946); Peter H. Kang (40,350); Ronald J. Meetin (29,089); Ken John Koestner (33,004); Omkar K. Suryadevara (36,320); David T. Millers (37,396); Kent B. Chambers (38,839); Michael P. Adams (34,763); Robert B. Morrill (43,817); Michael J. Halbert (40,633); Gary J. Edwards (41,008); William B. Tiffany (41,347); James E. Parsons (34,691); Daniel P. Stewart (41,332); Philip W. Woo (39,880); John T. Winburn (26,822); Tom Chen (42,406); Fabio E. Marino (43,339); William W. Holloway (26,182); Don C. Lawrence (31,975); Marc R. Ascolese (42,268); Carmen C. Cook (42,433); David G. Dolezal (41,711); Roberta P. Saxon (43,087); Bernice Chen (42,403); Mary Jo Bertani (42,321); Dale R. Cook (42,434); Sam G. Campbell (42,381); Matthew J. Brigham (44,047); Hugh H. Matsubayashi (43,779); Margaret M. Kelton (44,182); Joseph T. VanLeeuwen (44,383); Patrick D. Benedicto (40,909); T.J. Singh (39,535); Shireen Irani Bacon (40,494); Rory G. Bens (44,028); George Wolken, Jr. (30,441); John A. Odozynski (28,769); Cameron K. Kerrigan (44,826); Barmak S. Sani (45,068); Kenneth C. Brooks (38,393); Paul E. Lewkowicz (Reg. No. 44,870); and Theodore P. Lopez (44,881).

Please address all correspondence and telephone calls to:

Sam Campbell  
Attorney for Applicant(s)  
**SKJERVEN, MORRILL, MacPHERSON, FRANKLIN & FRIEL LLP**  
25 Metro Drive, Suite 700  
San Jose, California 95110-1349

Telephone: 408-453-9200  
Facsimile: 408-453-7979

I declare that all statements made herein of my own knowledge are true, all statements made herein on information and belief are believed to be true, and all statements made herein are made with the knowledge that whoever, in any matter within the jurisdiction of the Patent and Trademark Office, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be subject to the penalties including fine or imprisonment or both as set forth under 18 U.S.C. 1001, and that violations of this paragraph may jeopardize the validity of the application or this document, or the validity or enforceability of any patent, trademark registration, or certificate resulting therefrom.

Inventor's Signature: Steve A. F...

Date: 12/3/99

Post Office Address: 3996 Lyman Road  
Oakland, California 94602-1857

Citizenship: United States

Full name of second inventor: Sarkar, Shantanu

Inventor's Signature: Shantam Sam

Date: 12/3/99

Residence: San Jose, California

Post Office Address: 3381 Thrift Place  
San Jose, Claifornia 95148

Citizenship: India